Diebold Nixdorf

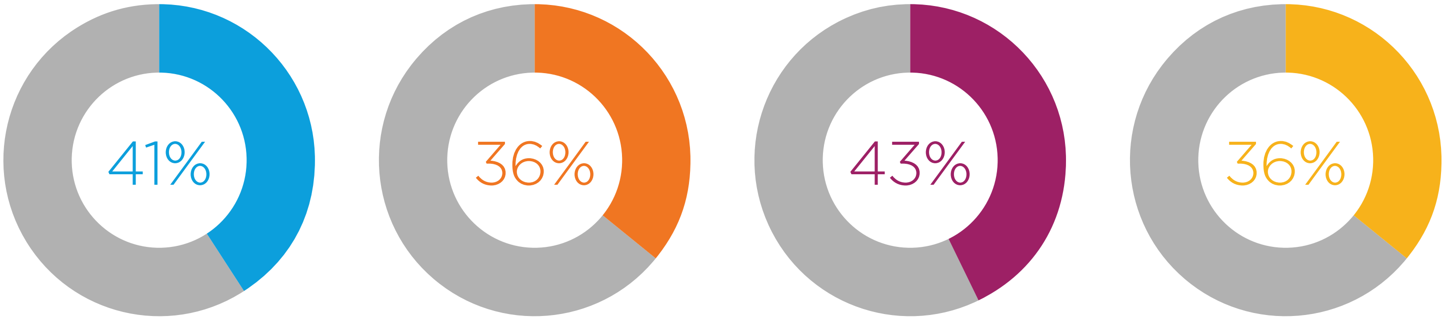
Diebold Nixdorf Comprehensive Security

Security and Software Updates: You Can’t Have One Without the Other.

Fact: PCI Requirement 6.1 states that every institution must ensure their system components and software are protected from known vulnerabilities by having latest vendor-supplied security patch installed—and speed is critical. PCI recommends installations of new security patches take place within one month of release.

The reality is … banks' network management processes often look very different "on the ground" from the aspirational (yet required!) recommendations from PCI. Many financial institutions don't adhere to this very important PCI requirement, which means their network is not compliant—and their terminals are at risk of attack. At best, this could translate to unnecessary fines for noncompliance … at worst, it could mean battling a breach in security and opening data and assets up to cyber attacks.

Figure 1



41% of FIs manage their own compliance updates in-house.

36% of FIs conduct weekly software updates/patches implemented across their ATM fleet.

43% of FIs conduct monthly software updates/patches implemented across their ATM fleet.

36% of FIs conduct on-site installation of updates either using internal staff or an outside vendor.

Figure 1 Source: Commissioned study conducted by Forrester Consulting on behalf of Diebold, November 2015

Why Are Software Security Updates So Difficult to Manage?

Modern self-service networks have evolved into complex webs of hardware and software that can be nearly impossible for financial institutions to keep straight and view holistically.

More than 100 utilities and drivers are stored on an ATM to make it run (i.e. Java, print drivers, AFD, etc.). Additionally, there are software maintenance updates and hot fixes for the different layers of software including XFS and the terminal application, as well as the operating system.

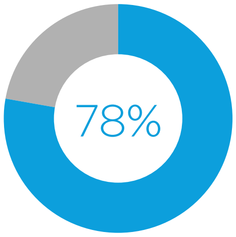
The 30-Day Rule: According to PCI, ALL the updates listed above must be made within 30 days of release to remain compliant.

The reality is ... many FIs find it incredibly challenging to maintain an accurate, up-to-date inventory of their entire self-service network (including hardware, software and configurations). The struggle is real: Keeping track of a self-service fleet that contains units purchased at different times, units from different manufacturers, units that have upgraded devices like printers, accepters, EPP, etc., and units that don't, different software stacks and different configurations, all with different recent service histories.

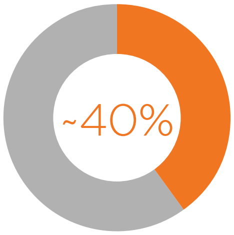
ATM Operators: When one terminal logs a maintenance call—and the software or a device is updated on that one machine, how are you tracking that information?

Unfortunately nearly four out of five FIs track these assets and changes manually—or not at all. These terminals and networks are running 24/7—and unless the tools securing them are operating on the same schedule, they're at extreme risk of being compromised.

Figure 2



78% of FIs either track fleet assets manually, rely on hardware vendors or simply don't have a good picture of their ATM inventory.



An estimated 40% of the total ATM market remain on Microsoft® Windows® XP, despite end of support and latent compliance issues.

PCI-DSS requires files to be reviewed for malicious events and tracked historically by who accessed the system and what they did there.

$5.5 BILLION

The industry has spent an estimated $5.5 billion over the past decade in operational costs just to keep pace with needed technology updates.

Figure 2 Sources: 2015 ATM and Self-Service Software Trends | ATIMA 2016 | PCI DSS Requirements and Security Assessment Procedures, Version 2.0
ATM Industry Association's 2014 Industry Overview

In an “Always On” World, the Stakes Are Higher Than Ever.

Emerging global threats, like jackpotting and other innovative new malware attacks, target ATM networks ruthlessly—but there are ways to protect self-service terminals comprehensively.

Jackpotting: Scammers install malware on a self-service terminal’s computer governing the cash dispenser, and command it to release all of the cash inside the terminal. It usually requires breaking into the machine, and requires in-person access.

ATM jackpotting is not a new problem, but it was relatively unheard of in the U.S. until mid-2017. Our security experts found that during recent jackpotting events, ATMs without the latest security patches were the most vulnerable to attack. In fact, during a six-month time frame, Diebold Nixdorf released seven security patches to insure our clients remained protected.

The patches, delivered via extensions for Financial Services (XFS), provided updates to the firmware on the dispenser board and were capable of stopping at least 30% of known jackpotting attacks. In addition, we advised our customers to physically change their software configuration and encrypt their hard drives as additional measures to counteract jackpotting efforts.

The reality is ... those updates only work if they’re installed—which is why it’s so critical to install patches **as soon as they become available.** Waiting 30 days—or even longer—is simply not good enough.

54%

More than half of the ATM industry experts who answered a recent survey agreed that Malware attacks are one of the top three threats facing the ATM industry in their region over the next five years.

$4 MILLION

Between May 2017 and January 2018, a crime ring stole $4 million during approximately 125 ATM attacks, according to the FBI.

Figure 3

Figure 3 Source: ATM Thieves Hit the Jackpot, Bloomberg Businessweek
https://www.bloomberg.com/news/articles/2018-07-02/atm-thieves-hit-the-jackpot

Modern ATM Fleets Require Modern Updating Techniques.

Centralized management is key to maintaining control over the increasingly complex ATM ecosystem. Remote administration and maintenance can help simplify processes, increase efficiency, and significantly reduce the total cost of ownership (TCO).

Best Practices for Successful Fleet Management

Performing regular audits is the first step to take. Regardless of whether your network is five devices or 50,000, the effort to constantly update and keep a record of current configurations can be exhausting—especially if your network is composed of different makes and models. But regular audits are key to identifying and addressing gaps in security and compliance.

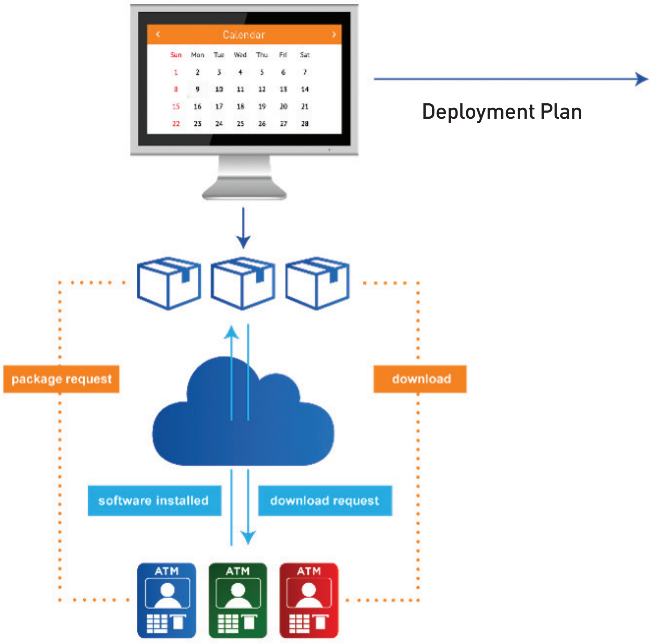
It's critical to keep your software stack up to date. The best way to move toward the ideal, fully compliant and protected state is to strategically deploy software updates from a single centralized console. Scheduling distributions at timely intervals (as opposed to once a quarter or even less frequently) ensures devices retain optimal uptime. More frequent updates also provide the peace of mind that PCI requirements are satisfied.

Optimize network traffic with distribution packages that use intermediate file servers.

- Cascade servers, building unlimited hierarchy levels for more efficient throughput and installation time.
- Distribute updates on demand or through scheduled events.
- Distribute software on single devices, through a hierarchy or across groups of devices.

Reduce physical visits to decrease maintenance costs.

- Accurately target specific versions of software configurations for upgrades.
- Plan maintenance and upgrades strategically to the entire channel.
- Dispatch all levels of the software stack or just individual components (see Fig. 1).



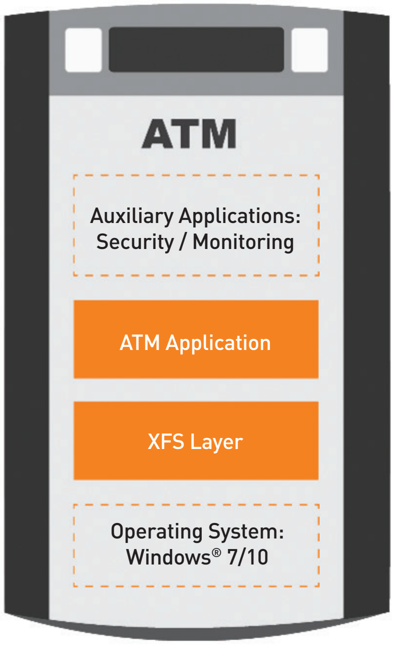

ATM
Auxiliary Applications: Security / Monitoring
ATM Application
XFS Layer
Operating System: Windows® 7/10

Figure 1:
Deploy remote software updates one layer at a time, or update the entire software stack.

What Does a Holistic View Look Like?

Every detail, every terminal, everywhere.

Regardless of whether your network is five devices or 50,000, the effort to constantly update and keep a record of current configuration can be exhausting—especially if your network is composed of different makes and models. Plus, IT resources are required to implement and maintain an updated software platform, and those same resources are often tasked with simultaneously addressing increased security threats as well as regulatory and compliance requirements. Vynamic View Inventory Manager streamlines the information into one “single source of truth” that offers ATM Ops teams the up-to-date information they need to stay compliant and keep things running smoothly.

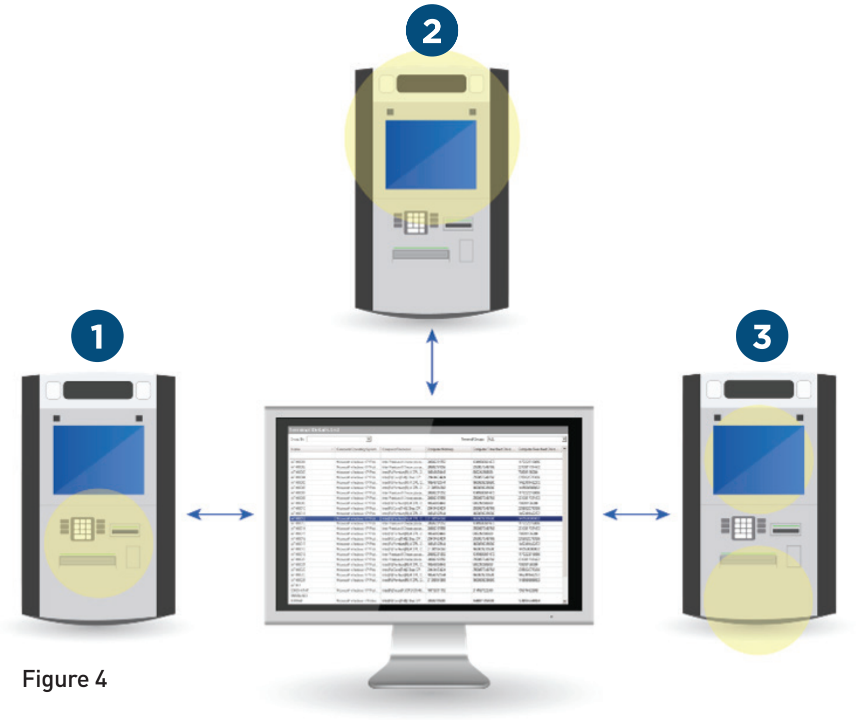
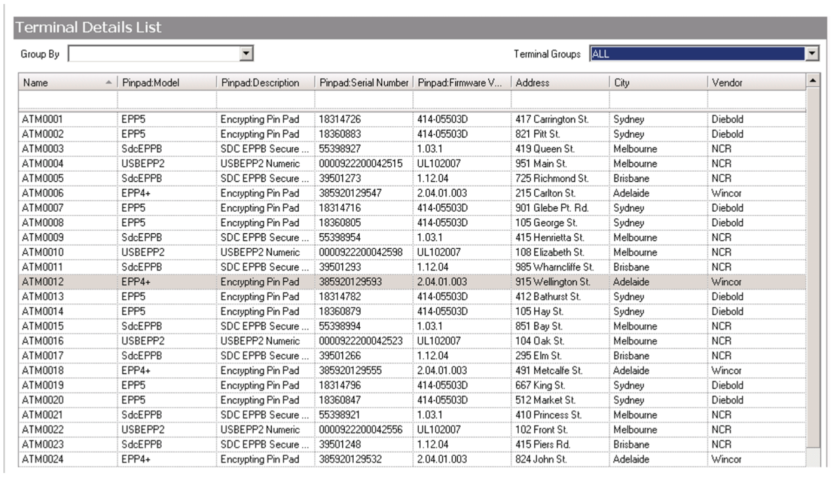


Figure 4

1 Track Details:
- Card reader
- Cash dispenser
- Pin pad
- Cash and check acceptors
- Envelope depositors
- Sensors

2 Manage Software Components:
- Publisher
- Version
- Description

3 Maintain Hardware Information:
- Processor
- Hard drive, memory
- Video card
- Monitor
- BIOS
- Sensors



Terminal Details List

Group By:

Terminal Groups: ALL

Name	Pinpad:Model	Pinpad:Description	Pinpad:Serial Number	Pinpad:Firmware V...	Address	City	Vendor
ATM0001	EPP5	Encrypting Pin Pad	18314726	414-05503D	417 Carrington St.	Sydney	Diebold
ATM0002	EPP5	Encrypting Pin Pad	18360883	414-05503D	821 Pitt St.	Sydney	Diebold
ATM0003	SdcEPPB	SDC EPPB Secure ...	55398927	1.03.1	419 Queen St.	Melbourne	NCR
ATM0004	USBEPP2	USBEPP2 Numeric	0000922200042515	UL102007	951 Main St.	Melbourne	NCR
ATM0005	SdcEPPB	SDC EPPB Secure ...	39501273	1.12.04	725 Richmond St.	Brisbane	NCR
ATM0006	EPP4+	Encrypting Pin Pad	385920129547	2.04.01.003	215 Carlton St.	Adelaide	Wincor
ATM0007	EPP5	Encrypting Pin Pad	18314716	414-05503D	901 Glebe Pt. Rd.	Sydney	Diebold
ATM0008	EPP5	Encrypting Pin Pad	18360805	414-05503D	105 George St.	Sydney	Diebold
ATM0009	SdcEPPB	SDC EPPB Secure ...	55398954	1.03.1	415 Henrietta St.	Melbourne	NCR
ATM0010	USBEPP2	USBEPP2 Numeric	0000922200042598	UL102007	108 Elizabeth St.	Melbourne	NCR
ATM0011	SdcEPPB	SDC EPPB Secure ...	39501293	1.12.04	985 Wharncliffe St.	Brisbane	NCR
ATM0012	EPP4+	Encrypting Pin Pad	385920129593	2.04.01.003	915 Wellington St.	Adelaide	Wincor
ATM0013	EPP5	Encrypting Pin Pad	18314782	414-05503D	412 Bathurst St.	Sydney	Diebold
ATM0014	EPP5	Encrypting Pin Pad	18360879	414-05503D	105 Hay St.	Sydney	Diebold
ATM0015	SdcEPPB	SDC EPPB Secure ...	55398994	1.03.1	851 Bay St.	Melbourne	NCR
ATM0016	USBEPP2	USBEPP2 Numeric	0000922200042523	UL102007	104 Oak St.	Melbourne	NCR
ATM0017	SdcEPPB	SDC EPPB Secure ...	39501266	1.12.04	295 Elm St.	Brisbane	NCR
ATM0018	EPP4+	Encrypting Pin Pad	385920129555	2.04.01.003	491 Metcalfe St.	Adelaide	Wincor
ATM0019	EPP5	Encrypting Pin Pad	18314796	414-05503D	667 King St.	Sydney	Diebold
ATM0020	EPP5	Encrypting Pin Pad	18360847	414-05503D	512 Market St.	Sydney	Diebold
ATM0021	SdcEPPB	SDC EPPB Secure ...	55398921	1.03.1	410 Princess St.	Melbourne	NCR
ATM0022	USBEPP2	USBEPP2 Numeric	0000922200042556	UL102007	102 Front St.	Melbourne	NCR
ATM0023	SdcEPPB	SDC EPPB Secure ...	39501248	1.12.04	415 Piers Rd.	Brisbane	NCR
ATM0024	EPP4+	Encrypting Pin Pad	385920129532	2.04.01.003	824 John St.	Adelaide	Wincor

Figure 5

Figure 4:
Vynamic™ View Inventory Manager provides a comprehensive central record system that intuitively, efficiently manages and tracks (in real time) the finest details of a self-service fleet. It's easy to track, search and maintain accurate records for your devices.

Figure 5:
Vynamic™ View Inventory Manager detail screen

How Can DN Deliver a Seamless Software-Management Solution?

The right partner offers strategic, end-to-end support that identifies security gaps—and has the tools and expertise to manage them.

STEP 1: We'll Evaluate Your Network

A successful security plan includes a thorough evaluation of the entire self-service network, including systems and software risk tolerance. By looking at a fleet holistically through a comprehensive audit conducted by our DN Professional Services experts, we evaluate your network from a complete configuration and security standpoint to ensure nothing falls through the cracks now or in the future.

Step Two: Upgrade the Low-Hanging Fruit

Our solutions are scalable and modular, designed to move self-service networks toward real-time analysis capabilities—on a customized timeline designed for each client individually. That could mean new software and/or service implementations, establishing connection points for remote software delivery, and enabling enhanced protection for emerging security threats. The ultimate goal is a comprehensive, real-time, 360° view of each terminal configuration.

Step Three: Prepare for the Future

As we upgrade software, services and processes to enhance security and maintain compliance now, we also work with our clients to build an action plan for the next phase of the self-service journey, whether that's implementing Windows 10 or preparing to install new terminals.

No matter where your network is located, its size or its reach, thieves are sizing it up to determine its weak spots. We'll help you develop an ironclad security strategy built on flexible, modular, integrated software, services and hardware that ensure your data—and your consumers—won't be compromised.

Protection You Can See.

With enhanced visibility across the entire self-service fleet, from the smallest details to the biggest software updates, you can minimize the opportunities for attacks.

DN Vynamic™

DN Vynamic software **empowers your organization to manage your self-service fleet holistically, comprehensively, and with the 360° view** required to stay on top of compliance and ensure maximum uptime.

Vynamic™ View offers a suite of software tools that are highly flexible and operate under a "think big, start small" philosophy. We collaborate with you to determine an action plan that meets your organization's individual priorities.

Each module in the Vynamic View suite provides one more piece toward building a network with full "Availability of Things." Your organization can build on the monitoring capabilities, using reporting and Business Intelligence (BI) to ensure that the software installed in your devices is up to date, pull more insightful information on the fleet components and drive a more comprehensive operation:

- **Software Deployment:** Automate software distribution and schedule software updates.
- **Inventory Management:** Automatically collect and report on installed software, firmware and hardware of any monitored device.
- **Availability Monitoring:** Receive remote status updates and notifications for real-time problem detection.
- **Incident Reporting:** Automate the ticketing process and track service calls.
- **Security Monitoring:** Detect if a device or transaction could potentially be fraudulent.
- **Log & Journal File Handling:** Efficiently collect, store and retrieve log files in near real-time.
- **Business Intelligence:** Leverage data from events throughout the fleet for analysis and optimization of business priorities.

DN AllConnect Services℠

DN AllConnect Services ensures your network stays up and running 24/7, 365 days a year, with service **provided by a global team of experts in self-service management.**

An initial engagement with DN Professional Services can audit your entire self-service fleet, providing your organization with a baseline assessment of the current situation, including gaps and weak spots that should be prioritized.

DN AllConnect Self-Service Fleet Management and Software Lifecycle Management services provide an integrated approach to managing the self-service fleet software stack, from design-driven development to active maintenance and management of the software lifecycle.

Software Lifecycle Management offers a standardized process framework that includes:

- **Requirements management**
- **Functional specifications and evaluation**
- **Implementation**
- **Release planning**
- **Testing**
- **Deployment**

And all of it is governed by Diebold Nixdorf as a single point of responsibility.

No two financial institutions' security needs or priorities are the same—so work with a partner that can scale flexibly and offer the modular solutions that meet your needs today, while building the foundation to grow securely into the future. Integrated, embedded security solutions give your network the edge it needs to stay secure against whatever attack comes next.

To learn more, **contact your Diebold Nixdorf representative or visit DieboldNixdorf.com.**